AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH AND SEIZURE WARRANTS

I, Jason Rameaka, do under oath depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Food and Drug Administration, Office of Criminal Investigation ("FDA-OCI") and have been so employed since August of 2013. I was previously employed as a Special Agent with the Criminal Investigation, Internal Revenue Service, United States Department of the Treasury, since April of 2000. I have attended numerous federal agency sponsored training courses as well as courses at the Federal Law Enforcement Training Center focused on financial investigations, food and drug law, federal narcotics violations, money laundering, and various other topics. I am assigned to OCI's Cybercrime Investigations Unit and am familiar with the tactics, methods, and techniques of persons who unlawfully market and distribute drugs via internet websites.

2. As a Special Agent with FDA/OCI, I am responsible for conducting criminal investigations involving violations of the Federal Food, Drug, and Cosmetic Act ("FDCA"), Title 21, United States Code, Section 301, et seq., and other federal statutes enforced by the United States Food and Drug Administration ("FDA"). I have also assisted in search, seizure, and arrest warrants in numerous financial and asset forfeiture investigations. I have been involved in the effect of seizures of assets, currency, and other property under 18 U.S.C. §§ 981 and 982.

3. The information contained in this affidavit comes from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show solely that there is sufficient probable cause for the requested search

warrant. While I have set forth all material information pertinent to the requested search warrant, the affidavit does not include all of my knowledge about this matter.

PURPOSE OF THE AFFIDAVIT

4. This affidavit is submitted in support of a search warrant for the following electronic devices seized from George Kuiper ("G. KUIPER") at 333 Summit Ridge Drive, Lawrenceville, Georgia ("the Subject Premises"), and currently located at the Norris Cotton Federal Building, 275 Chestnut Street, Manchester, New Hampshire (together, "the Devices"). The Devices are more fully described in Attachment A attached hereto and incorporated herein. The devices include:

a. one LG Brand flip phone;

b. one HP Compaq Elite 8300 Desktop Computer with serial number MXL250153W; and

c. two USB drives evidence number 09-0373-42156 one of which is labeled "Wincleaner" and one of which is labeled "rabbitTV."

5. As is set forth in detail below, I submit that there is probable cause to believe that G. KUIPER has utilized the Devices to engage in money laundering and operating an illicit pharmacy business and/or that evidence of those crimes will be found on the Devices. Consequently, I submit there is probable cause to search the Devices for instrumentalities, fruits, and evidence of the commission of crimes including, violations of violations of Title 21, United States Code, §§ 331(a), 331(d) (introduction of misbranded and unapproved new drugs into interstate commerce), 841(a), 846, (distribution and conspiracy to distribute controlled substances) 952(b), and 963 (unlawful importation of controlled substances), and Title 18,

United States Code, §§ 371 and 545 (conspiracy and importation contrary to law), 1957, 1956(a)(2), and 1956(h) (money laundering).

APPLICABLE STATUTES

6. Under the FDCA, the term "drug" includes articles which are intended (1) for use in the diagnosis, cure, mitigation, treatment, or prevention of diseases in man or (2) to affect the structure or any function of the body of man. 21 U.S.C. § 321(g)(1)(B) and (C).

7. Under the FDCA, the term "new drug" includes any drug that is not generally recognized, among experts qualified by scientific training and experience to evaluate the safety and effectiveness of drugs, as safe and effective for use under the conditions prescribed, recommended, or suggested in the labeling thereof. 21 U.S.C. § 321(p)(1).

8. With limited exceptions not applicable here, unless the FDA has approved a new drug application or an abbreviated new drug application, new drugs are "unapproved" and cannot lawfully enter into interstate commerce. In other words, introducing or causing the introduction into interstate commerce of a new drug that does not have an FDA-approved application, i.e. an "unapproved" new drug, is generally prohibited. 21 U.S.C. §§ 355(a) and 331(d).

9. Under the FDCA, certain drugs, because of their toxicity and other potential harmful effects, are not considered safe for use except under the supervision of a practitioner licensed by law to administer such a drug. Those drugs, as well as drugs approved by FDA for use only under the supervision of a licensed practitioner, are known as prescription drugs. 21 U.S.C. § 353(b)(1).

10. Prescription drugs may be dispensed only upon the prescription of a licensed practitioner. 21 U.S.C. § 353(b)(1). Dispensing a prescription drug without the prescription of a licensed practitioner causes a drug to be "misbranded." *Id*. Introducing a misbranded drug into

interstate commerce or causing the introduction into interstate commerce of any misbranded drug is prohibited. 21 U.S.C. § 331(a). The FDCA imposes strict-liability misdemeanor punishment for violations of 21 U.S.C. §§ 331(a) and 331(d). 21 U.S.C. § 333(a)(1); *United States v. Park*, 421 U.S. 658 (1975). The FDCA imposes felony punishment for violations committed with the "intent to defraud or mislead." 21 U.S.C. § 333(a)(2).

11. Certain prescription drugs are also classified as "controlled substances" under the Controlled Substances Act (hereinafter "CSA") and are subject to regulation under that statue. "Schedule IV" controlled substances, as defined by statute, include drugs determined to have accepted medical use in treatment in the U.S. and the abuse of which could lead to a limited physical dependence relative to drugs and controlled substances in other schedules. 21 U.S.C. § 812(b)(4).

12. The CSA contains its own prohibition on dispensing of prescription drugs that are also Schedule IV controlled substances except upon the prescription of a licensed practitioner. 21 U.S.C. § 829(b). Additionally, Schedule IV controlled substances cannot be distributed or generally handled in the course of being distributed other than by persons and entities registered with the United States Drug Enforcement Administration (hereinafter "DEA"). 21 U.S.C. § 822.

13. The importation of prescription drugs into the United States is subject to laws and regulations administered by United States Customs and Border Protection, and the FDA, and, in the case of controlled substances, the DEA. Among other things, a prescription drug may be lawfully imported into the United States only if it is approved by the FDA or exempt from approval. 21 U.S.C. § 331(d).

14. In addition, under the CSA, it is unlawful to import, or to conspire to import, into the United States a non-narcotic Schedule IV controlled substance unless the controlled

substance is imported for medical, scientific, or other legitimate uses and pursuant to notifications and declarations prescribed by regulation. 21 U.S.C. §§ 952(b) and 963.

15. It is a crime for any person to fraudulently or knowingly import or bring into the United States any merchandise contrary to law. 18 U.S.C. § 545. Any importation of a drug in violation of the CSA or the FDCA constitutes an importation contrary to law.

16. It is a crime to manufacture, distribute, dispense or possess with intent to distribute controlled substances, or to conspire to do the same, unless authorized by the CSA and its regulations. 21 U.S.C. §§ 841(a) and 846.

17. Knowingly or intentionally delivering, distributing, or dispensing a controlled substance by means of the internet by an online pharmacy that is not validly registered to engage in such internet activity is a crime. 21 U.S.C. § 841(h)(1).

18. Under 18 U.S.C. § 1956, a violation occurs when an individual, knowing that the property involved in a financial transaction represents the proceeds of unlawful activity, conducts or attempts to conduct a financial transaction with proceeds of specified unlawful activity with the intent to promote the carrying on of the specified unlawful activity or knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership or control of the proceeds of specified unlawful activity. In addition, an individual violates Section 1956 when he or she transports, transmits, or transfers, or attempts to transport funds from a place inside the United States to a place outside the United States with the intent to promote the carrying on of specified unlawful activity, or knowing that that the funds involved in the transportation represents the proceeds of specified unlawful activity that are designed to conceal the nature, location, source, ownership or control of the funds, is in violation

of 18 U.S.C. § 1956. It is also unlawful to conspire to make such transmissions or transfers. 18 U.S.C. § 1956(h).

19. Under 18 U.S.C. § 1957, a violation occurs when an individual knowingly engages or attempts to engage in a monetary transaction in criminally derived property that is of value greater than $10,000 and is derived from specified unlawful activity.

20. Under 18 USC § 981, any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. §§ 1956, or 1957 is subject to civil forfeiture to the United States.

21. Under 18 U.S.C. § 982, any property, real or personal, involved in or traceable to a violation of 18 U.S.C. §§ 1956 or 1957 is subject to criminal forfeiture.

22. The proceeds of Controlled Substance offenses are forfeitable pursuant to Title 21 U.S.C. Section 853(a)(1) and 881(a)(6).

23. Title 18, U.S.C. Section 984 provides that fungible property such as cash, monetary instruments in bearer form, or funds in a financial institution, whether or not directly traceable to an offense, may be subject to forfeiture up to one year from the date of the offense. This section does not limit the ability of the United States to forfeit property that is directly traceable to the offense. 18 U.S.C. § 984(d).

24. 18 U.S.C. § 981(b), the civil forfeiture statute authorizing the seizure of property subject to forfeiture, requires a showing of probable cause, but does not require a showing that less restrictive means may not be sufficient to secure the funds.

25. The criminal seizure warrant statute, 21 U.S.C. § 853(f), requires the court to determine that a restraining order, an injunction, or a temporary restraining order as provided by 21 U.S.C. § 853(e), may not be sufficient to assure the property for forfeiture.

26. The Court is entitled to infer from the inherent fungibility and transferability of money in a bank account that a restraining order under section 853(e) would be inadequate. *United States v. Swenson*, 2013 WL 3322632 (D. Idaho July 1, 2013); *United States v. Wiese*, 2012 WL 43369, *2 (E.D. Mich. Jan. 9, 2012); *United States v. Martin*, 460 F. Supp. 2nd 669, 677 (D. Md. 2006), aff'd 662 F. 3d 301, 304 n.6 (4th Cir. 2011).

27. "There is no requirement under § 853(f) in particular, or in any seizure warrant in general, and the court has located no case to the contrary, that the Judicial Officer issuing the seizure warrants is required explicitly to state that a restraint under § 853(e) may not have sufficiently assured the availability of funds." *United States v. Wiese*, 2012 WL 43369, *2 (E.D. Mich. Jan. 9, 2012).

PROBABLE CAUSE

28. I am currently investigating G. KUIPER and his associated websites New.nubrain.com, Nubrain.com, and Healthclown.com for violations of the statutes described herein. I believe G. KUIPER resides at and operates an unlawful business out of the Subject Premises.

29. According to FDA-OCI records, Nubrain.com was the subject of a previous investigation around the year 2000. As part of the investigation, investigators interviewed G. KUIPER. According to a report of the interview, G. KUIPER said that he was the founder/owner of a company called Cosmic Sales and Marketing, Inc. which sold vitamins and health products. In 1996 or 1997, he launched the website Nubrain.com. He said that most of the products he sold were Nootropics, or non-prescription pharmaceuticals related to the enhancement of memory and mental well-being. He admitted that some of the drugs he sold required a prescription and acknowledged that he never required one to sell the drugs on the website. He said that the drugs

he sold were shipped from suppliers located overseas directly to his customers in the United States or first to himself at his Lawrenceville, Georgia post office box. In November of 2001, G. KUIPER's attorney sent FDA/OCI a letter saying that G. KUIPER had stopped selling prescription drugs immediately after being interviewed. Investigators reviewed the website and confirmed that prescription drugs were no longer available. The investigation was therefore suspended at that time.

30. The investigation was reopened in 2009 after FDA/OCI received information from a Maine Police Department that someone had purchased unapproved prescription drugs from the website Nubrain.com. The drugs were shipped with a return address of a post office box rented by G. KUIPER. At that time, the website Nubrain.com was registered to "Nubrain" and listed as its administrative contact G. KUIPER of Cosmic Sales and Marketing. Further, according to the registrar for the domain Nubrain.com, in October 2010, this website was associated with G. KUIPER and the Subject Premises.[1]

Controlled Purchases and Identification of G. KUIPER's Websites

31. After reopening the investigation in 2009, on eight occasions detailed below, FDA agents purchased modafinil,[2] a Schedule IV controlled substance and prescription drug not approved by the FDA, and other drugs from Nubrain.com and other websites operated by G. KUIPER. The purchases never required a prescription.

32. In September 2009, the website nubrain.com claimed to be a U.S. based company that had been distributing smart drugs and health products since 1981. The website's homepage

[1] The domain registration information subsequently changed and as of December 17, 2014, Nubrain was registered to "Perfect Privacy, LLC" located in Jacksonville, Florida. According to its website, Perfectprivacy.com offers private domain registration by substituting its own contact information for the contact information of the domain name owner, so the domain name owner's information does not appear on registration searches.

[2] Modafinil has been classified as a Schedule IV Controlled Substance since 1999.

declared it, "Your Source for Smart Drugs/Nootropics" and had over 100 products for sale. Nubrain.com was not registered with the DEA to distribute, or handle in the course of being distributed, controlled substances.

33. On April 29, 2009, an agent acting in an undercover capacity established an account with Nubrain.com and placed an order for two prescription drugs, Modafinil and Olmifon (Adrafinil). No prescription was required, no medical questionnaire was administered, and no consultation with a medical practitioner occurred prior to or after placing the order. The agent received a confirmation email from Nubrainorders@yahoo.com, an email account still used to communicate with customers as recently as May 2020. On May 4, 2009, the undercover agent received a package with the return address of NUBRAIN, PO Box 1364, Lawrenceville, GA 30046 USA.[3] The package contained the two drugs ordered. The Olmifon box and package insert were both in foreign writing and the Modafinil box was labeled with a warning that it can only be provided with a prescription.

34. In June 2009, October 2009, and May 2012, the undercover placed additional orders from Nubrain.com. Each time, the agent received a package with the same return address including drugs that were not approved by the FDA for distribution in the United States. He was never asked to provide medical information.

35. On November 4, 2013, an agent accessed a different website, New.Nubrain.com and placed an order for Modafinil. No prescription or medical questionnaire was required and no consultation with a medical practitioner occurred prior to or after placing the order. On November 15, 2013, a parcel was received containing pills marked "Modalert 200 Modafinil tablets" and identifying the manufacturer as "Sun Pharma" of India. The return address on the

[3] All of the drugs purchased during controlled purchases discussed in this affidavit were sent to an FDA/OCI monitored P.O. box in New Hampshire.

package was the same return address as the previous parcels. Modalert is not approved by the FDA for distribution in the United States.

36. By on or about February 17, 2015, www.nubrain.com and new.nubrain.com were no longer accessible. Unbeknownst to agents conducting this investigation, on February 17, 2015, another member of FDA/OCI had sent Web.com a list of domain names registered through Web.com that OCI believed were unlawfully selling drugs. Among the domain names on the list were nubrain.com. A subsequent review of G. KUIPER's emails received pursuant to a search warrant revealed that Web.com revoked the registration of Nubrain.com on February 17, 2015, for violating Web.com's terms of service.

37. The same day this happened, G. KUIPER sent an email to Ecbuzz.com stating, "my website has been suspended[.] [I] am going to create and register a new domain name will you be able to transfer all existing files to the new domain once I have it set up?" According to its website, Ecbuzz.com provides website development services and is located in Pune, India. On February 18, 2015, G. KUIPER made a request to register the domain name Healthclown.com and requested that the site be registered to Carolina Hincapie, Calle 32 #222, Medillin, Columbia, using caro.k2@hotmailcom as the contact email address.[4]

38. On November 11, 2016, agents accessed Healthclown.com, which was nearly identical in appearance to Nubrain.com. Healthclown.com is not registered with the DEA to distribute, or handle in the course of being distributed, controlled substances. The website offered a product for sale called "Smart Combo 200/90" under the category "Smart

[4] According to Western Union records, G. KUIPER has sent numerous wire transfers to Carolina Hincapie Saldarriaga in Columbia. On various wire transfers, the email account associated with George Kuiper was nubrainstore@yahoo.com and the email account associated with Carolina Saldarriaga was caro.k2@hotmail.com. According to emails reviewed pursuant to a search warrant, G. KUIPER described Hincapie Saldarriaga on one occasion, as "…our secretary and is on vacation with her family" and on another occasion as "…my wife…". I have not been able to confirm whether G. KUIPER is in fact married to Hincapie Saldarriaga.

Drugs/Nootropics." Although the product was not specifically identified as modafinil, the product image on the Healthclown.com website was similar to that used for drugs containing modafinil on the Nubrain.com website. Agents attempted to purchase the product by creating an account on the Healthclown.com website using an email address previously used on the Nubrain.com website. After entering the previously used information, an error message was received stating that there was already an account for the email address, prompting the agents to log in to the existing account. Agents were then able to successfully log on to Healthclown.com using the email address utilized during the prior undercover purchases from the Nubrain websites.

39. After logging onto the account on Healthclown.com, agents completed the purchase of the "Smart Combo 200/90" product. A few days later, agents received a package which contained 90 tablets of 200 mg Modalert, manufactured by Sun Pharma of India and labeled to contain 200mg of modafinil per tablet. According to the credit card statement for the credit card used for the purchase, the merchant for the purchase was listed as "Nubrain 770-339-9971."

40. On September 12, 2019, agents accessed Healthclown.com using the same account information. Agents then ordered 120 200mg Modalert tablets, among other products. No prescription or medical questionnaire was required, and no consultation with a medical practitioner occurred prior to or after placing the order. Shortly after placing the order agents received an email inquiring if they were a new customer, and if so, how they found the website. Agents replied to the email that they had ordered from the website in the past. Agents then received an email indicating that the order, "will go out tomorrow from Atlanta."

41. On or about September 20, 2019, agents received a parcel with a return address of PO BOX 397, Grayson, GA 30017. The parcel contained five blister packs each containing 10 individually wrapped Selegiline HCI tablets IP 5mg for a total of 50 pills, labeled "Manufactured by INTAS PHARMACEUTICALS LTD" in India and 12 blister packs each containing 10 individually wrapped Modafinil tablets 200mg for a total of 90 pills, labeled "Modalert 200 Manufactured in India by: sun pharma laboratories ltd."[5]

42. On or about April 9, 2020, agents accessed Healthclown.com using the same account information. Agents then ordered 120 200mg Modalert tablets, among other products. No prescription or medical questionnaire was required, and no consultation with a medical practitioner occurred prior to or after placing the order. Agents paid with a postal money order which was sent to Nubrain at P.O. Box 397 in Grayson, Georgia. The money order was signed and cashed by G. KUIPER.

43. On or about April 15, 2020, agents received an email from sales@healthclown.com informing them that the order would ship within 2-3 weeks. On that same date agents responded to said email and stated "2-3 weeks for shipping? You've never taken this long in the past." Shortly after sending the email agents receive a response from nubrainorders@yahoo.com stating: "ALL ORDERS ARRIVE FROM OVERSEAS the suppliers have shut down for the past month we will keep you updated"

44. On May 1, 2020, the undercover account received an email saying that the order status was "complete" but with a comment, "still waiting for supplier to resume shipping." The agent responded on May 5, 2020, "Can I order more so I can stock up and not have to wait so

[5] Agents paid with a credit card. According to records from the credit card company, the payment went to an account at Fifth Third Bank. I was not able to verify any account at that bank in the name of any entities associated with G. KUIPER.

long next time?" The agent then received a response that same day saying, "lets hold off and see how things develop with the supplier etc." On May 15, 2020, agents received another email saying, "as soon as shipper resumes we will let you know the problem is the flights leaving INDIA beyond control of supplier we are looking at another option." Agents have still not received the order.

Email & Web Hosting Search Warrants

45. In November 2009, March 2015, January 2017, and May 2020, a United States Magistrate Judge in the District of New Hampshire issued search warrants for email accounts associated with G. KUIPER and his associates.[6] In September 2015, the Court in the District of New Hampshire also issued a search warrant for a web hosting company, Liquidnet, that hosted domain names for Nubrain.com, New.Nubrain.com, and Healthclown.com.

46. Several database files were stored on Liquidnet servers and were produced in response to the search warrant. One database entitled "Nubrain Mycart" listed various drug sales totaling approximately $2.6 million for the time period 2006 through 2012. Of the $2.6 million in sales, almost $1.2 million were for sales of Modafinil. A second database file, entitled "Nubrain New," listed approximately $1.2 million in sales from 2012 through 2015, including sales from both the New.Nubrain.com and Healthclown.com websites. Of the $1.2 million in sales, approximately $875,000 were for sales of Modafinil. Invoices recovered from this search warrant listed various addresses including the Subject Premises.

Daily Website Operations

[6] On May 15, 2020, agents received the results of a search warrant for nubrainorders@yahoo.com which contained approximately 9,000 emails. I have not yet reviewed all of the emails. However, from my preliminary review, I have determined that KUIPER continues to use the email address to operate his illicit drug business, including take orders from customers, communicate with suppliers, and process payments for other companies in the illicit pharmacy business.

47. A review of emails and other information obtained from the above-referenced search warrants revealed that G. KUIPER has worked closely with his daughter, Liana Kuiper ("L. KUIPER"), and her mother, Claudia Vieira ("C. VIEIRA"), to sell prescription drugs without a prescription, to sell unapproved new drugs, and/or to illegally import and distribute controlled substances to customers throughout the United States and abroad.[7] Agents were able to identify all three and their relationship with each other based on a thorough review of emails they exchanged. For example, they sometimes sign their own names in the emails and refer to each other in ways that make clear they are related (e.g. L. KUIPER referring to C. VIEIRA and G. KUIPER as "mom" or "dad"). L. KUIPER also signs some emails, "Nubrain Shipping dept Liana K."

48. The three regularly discussed the illicit online pharmacy business. For example, an email dated June 23, 2014, from L. KUIPER to G. KUIPER, with the subject line "Ok to send?" included an attachment with information under the headings "MODALERT ORDERS 100mg June 23rd 2014" and "MODALERT ORDERS 200mg June 23rd 2014." The attachment, which appears to be ultimately intended for G. KUIPER's supplier, listed apparent customer drop-ship orders for Modalert. The attachment also included requests for apparent shipments of Modalert to VIEIRA at a post office box.

49. On August 27, 2014, G. KUIPER, using email nubrainorders@yahoo.com sent L. KUIPER an email at nubrainship@yahoo.com. The email included copies of emails between G. KUIPER and a supplier of modafinil drugs asking G. KUIPER to wire money to a bank in India

[7] On March 7, 2018, L. KUIPER was encountered by U.S. Customs and Border Protection (CBP) officers when she entered the U.S. at Atlanta, Georgia Airport. During a routine secondary inspection, L. KUIPER stated that she works for her father's business, indicating the business is an online pharmaceutical company named Cosmic Sales, and that her role is to take the orders and fill them. L. KUIPER advised that Cosmic Sales sells vitamins to elderly people with mental disabilities and that the top-selling vitamin was Modafinil. L. KUIPER further stated that her father is involved in other business ventures to include processing payments for elderly people.

as payment for previous orders. G. KUIPER's email stated, in relevant part, "you need to go to brand bank and send 3000 wire to this guy." L. KUIPER replied, "How ! What do you want me to do exactly. Mom will go tomorrow or Friday. Give me details." G. KUIPER responded "call me to discuss[.] [O]nly you can sign the wire."

50. In one email exchange in October 2016 between L. KUIPER, utilizing the email account Nubrainship@Yahoo.com, and G.KUIPER, utilizing the email account Nubrainorders@Yahoo.com, GEORGE KUIPER wrote, "…where is your mom? Why does she not answer her cell phone i am thinking of having freedom send their checks to the po box in Marietta instead of grayson then she can so [sic] the totals at home and mail the deposits to brand bank from Marietta and save all that time driving or maybe she can just come to brand bank once a week." L. KUIPER responded "I think it's a great idea to send checks to Marietta so mom has more work to do to keep her learning and busy. Can you start doing that and have her drive down to Lawrenceville once a week." According to DMV records, VIEIRA has at least two registered to her at an address in Marietta, Georgia (one of which is the Subject Vehicle, which G. KUIPER drives). The Subject Premises is in Lawrenceville. As will be discussed in more detail below, I believe that "freedom" refers to Freedom Pharmacy, an illicit pharmaceutical website that G. KUIPER works with. I have identified an account at Brand Bank (which is now Renasant Bank) that is used to facilitate the business.

51. G. KUIPER also regularly communicated with companies that ship drugs from overseas. For example, an email dated January 15, 2017, was sent to Shah and Company with the subject line "Modalert Orders 1/15/17 (2 ORDERS)." [8] The email instructed Shah and Company

[8] In an email to KUIPER in 2014, Shah claimed to have a website, Pharmacyexporter.com. According to an archived version of pharmacyexporter.com, Shah and Company was established in 2001 in Mumbai, India as a "…reputed Exporter of a wide range of medicines and pharmaceutical products…." In 2016, a search of HSI's Treasury Enforcement Communication System (hereinafter "TECS") revealed that five packages shipped by Shah

to ship 700, 200mg Modalert tablets to the following two addresses: D. Diaz, PO Box 397, Grayson, Ga 30017 and C. Vieira, PO Box 670913, Marietta, Ga 30066.

52. In addition, emails show that drugs were sent to G. KUIPER from other international suppliers as well, some of which were seized by customs officials. For example, in 2014, one email provided order and tracking numbers for four shipments sent from Fiji. According to law enforcement records, three of the four packages identified were seized. One package was shipped with a Customs Declaration Form describing the contents as "Body Care Products." The package, which was found to contain 600 Modafinil tablets, had been sent to GEORGE KUIPER, at the Subject Premises from Fiji. Another was shipped with a Customs Declaration Form describing the contents as "Body Care Products." The package, which was found to contain 600 Modafinil tablets, was shipped to GEORGE KUIPER, PO Box 465837, Lawrenceville, Georgia from Fiji. A seizure letter was sent to this address along with a registered receipt form addressed to G. KUIPER. G. KUIPER signed the receipt. The third package was found to contain 600 Modafinil tablets and was shipped to L. KUIPER, from Fiji. A seizure letter was sent addressed to L. KUIPER. VIEIRA signed the registered receipt. Each seizure letter stated that the items were seized for violation of Title 21, U.S.C., Section 952(b) and Title 21, C.F.R., Part 1312.11 because the items were controlled substances and the recipients did not comply with the import permit and declaration requirements.

53. On March 10, 2020, a customer emailed G. KUIPER a customs letter saying "[t]oday I received a letter from the Government saying they seized my back pills. With a letter stating that it is illegal to import meds into the USA." G. KUIPER, using

---

and Company of Mumbai, India were seized in 2015 by U.S. Customs and Border Protection because they were found to contain controlled substances.

Nubrainorders@yahoo.com responded, "about 5% of orders are seized we will replace the product from Atlanta as soon as we receive product you can throw away the letter." On March 24, 2020, a different customer emailed sales@healthclown.com saying "well it's official I got a notification from customs that I need to register with the DEA or they're going to destroy the products." Nuborainorders@yahoo.com responded, "please discard the letter. Will replace next week." On May 6, 2020, G. KUIPER discussed, over email, two parcels that had been shipped to a customer but never left customs. G. KUIPER told the customer, "it is unusual for 2 orders to be seized right after the other like this as seizures are random however, because of the current virus it may be that more parcels from overseas were examined that month…" I believe G. KUIPER likely referred to travel restrictions caused by the COVID-19 virus. In fact various emails, like the one received by the undercover agent discussed shipments being delayed from India because of the virus.

Payment Processing for Overseas Entities

54. Historically, G. KUIPER accepted several forms of payment for orders placed online including money orders, wire transfers, and credit card.[9] The merchant account processor utilized by G. KUIPER to process credit cards was First American Payment Systems. According to a Merchant Application & Agreement with First American signed by G. KUIPER on April 20, 2010, the business name G. KUIPER utilizes is Cosmic Sales and Marketing, Inc with a mailing/billing address of the Subject Premises and phone number of 770-339-9971. Further, the merchant name utilized by G. KUIPER on credit card transactions is "Nubrain."

55. According to a review of emails and banking records, G. KUIPER had a relationship with a company in the United Kingdom, Quality Health Incorporated ("QHI"),

[9] Recent emails suggest that he may have stopped taking credit cards (confirmed by the most recent undercover purchase which required a money order).

which utilized the website QHI.CO.UK. This website sold a variety of prescription drugs, including at least one drug that contains Modafinil.

56. Various emails confirm that Nubrain processed credit card orders on behalf of QHI. Specifically, on a consistent basis, QHI transmitted, via email, a listing of customer names, credit card numbers and order amounts, to Nubrain for processing. In exchange for processing these cards, Nubrain appeared to charge QHI 7.5% of each transaction and then transmitted funds to QHI via checks drawn on Nubrain's bank account. Emails indicate that G. KUIPER began to process credit card transactions on behalf of QHI because QHI was engaged in unlawful activities in the UK. For example, an email dated April 6, 2009, sent from a man named Brett Specter stated, "[t]he information I'm going to share with you now is VERY confidential but I want you to understand why I've instructed Tracy not to contact customers by phone unless they are very well known to us. The fact is that Quality Health would not be allowed to operate as a (normal) business in England or anywhere in Europe for that matter. If the authorities suspected that it was actually based (in country), they would shut it down immediately, possibly freeze bank accounts, etc., etc."

57. In December 2016 and again in October 2017, an HSI agent, acting in an undercover capacity, logged onto the QHI website and placed orders for Modafinil. On both occasions, drugs containing Modafinil were shipped from outside the U.S. to a location controlled by HSI in New Hampshire. On both occasions, the packages contained Customs Declaration Forms stating the packages contained "Documents" and provided a description of "Documents & Items For Personal Use." Finally, on both occasions, the credit card utilized to make the purchase listed the merchant on the credit card statement as "Nubrain 770-339-9971 GA." This was G. KUIPER's phone number and very similar to what appeared on credit card

statements for purchases the undercover agent made from G. KUIPER's websites. At that time, the QHI website explained, "[a]t this time all credit card orders will be charged by NUBRAIN in US dollars. They are based in the USA. This is the name that will appear on your credit card statement."

58. I am aware that the United Kingdom's Medicines & Healthcare products Regulatory Agency (MHRA) is actively investigating Brett Specter and his company QHI. After they executed a search, Specter shut down his business. Specter was interviewed by authorities and in a statement that he prepared dated January 16, 2019, he wrote, "Merchant banks tend not to wish to provide credit card facilities for non-national companies. Consequently I used third party processors and for the past approximate seven or eight years, George Kuiper of Nubrain Inc., located in the USA, provided QHI with the provision of credit card facilities. I chose Nubrain Inc. as I knew them to be an experienced, reputable and responsible company capable of securely providing the service to QHI."

59. I believe that G. KUIPER performed a similar service for at least one other internet pharmacy as well. Based on a tip, on October 9, 2014, agents accessed another internet pharmacy, Freedom-pharmacy.com. According to the website, it provides on-line access to over 5,000 pharmaceuticals in categories ranging from anxiety to weight loss. The site states that it is associated with Archipelago Suppliers of Port Vila, Vanuatu. Agents placed an order for a prescription drug. After providing billing and shipping information, agents selected to pay for the transaction utilizing a money order. Agents were then instructed to send the money order to Cosmic Sales, PO Box 1199, Grayson, Georgia. According to U.S. Postal records, in March 2013, this PO Box was assigned to Cosmic Sales and the person who applied for the box was G. KUIPER of the Subject Premises.

60. Agents accessed the website Freedom-pharmacy.bz on January 31, 2020 and found it to be substantially the same as the website visited in 2014. According to LegitScript, a company that contracts with FDA to provide internet monitoring services, Archipelago Suppliers which is still listed as affiliated with the website, is a rogue Internet pharmacy network with many affiliated websites selling prescription drugs without a prescription.

61. As recently as March 19, 2020, G. KUIPER was copied on an email from someone named "Eric" who wrote to "pharmacist@archipelagosuppliers.com" introducing "George" and describing him as a "friend who helps us with payments [and] has clientele that he services with modalert and other generic versions." The person using the Archipelago Suppliers email address then offered to ship modalert orders on behalf of G. KUIPER.

62. On or about September 30, 2019, G. KUIPER sent an email to a person with email address "Curtthurston@gmail.com" who I believe to be Curtis Thurston, discussing their agreement for G. KUIPER to process payments on Thurston's behalf. G. KUIPER told Thurston, "I decided NOT to accept credit cards anymore as I slowly winding down my business activity and that is a good start. Your US based customers can send a check (as most of mine do) reducing your fee from 8.3% to 5%." G. KUIPER than offered to contact "another US based smart drug company . . . to see if they would consider processing your cards as I have been doing." He signed the email "gk." In the same email exchange, Thornton wrote that G. KUIPER had processed "$37,684" in 2018. I believe Thornton operates an online pharmacy because in one email he wrote, "I was just about to add another drop-shipper for antibiotics and that could have taken sales even higher."

63. Bank records confirm that G. KUIPER has accepted payments from customers buying drugs from these other illicit online pharmacies. He then makes lump sum wire transfers back to these organizations, sometimes in excess of $10,000.

64. Agents issued a subpoena to Charter Communications for recent logins to the nubrainorders@yahoo.com email account and found that the IP address was subscribed to Lavanderia Jalisco, at an address in Lawrenceville, Georgia a few miles from the Subject Premises. Although most emails on the account are signed "George" or "gk" some are signed with the name "Steve."

65. According to the DEA, KUIPER, L. KUIPER, C. VIEIRA, Cosmic Sales & Marketing, Nubrain.com, and Healthclown.com are not registered as importers or distributors of controlled substances and therefore, cannot legally import or distribute controlled substances.

Search of the Subject Premises

66. On or about June 23, 2020, United States Magistrate Judge Regina Cannon issued a search warrant for the Subject Premises. The warrant authorized the seizure of electronic devices. On or about June 24, 2020, agents executed the warrant. Among other things, they seized one LG Brand flip phone which G. KUIPER indicated was his only cellular telephone, one HP Compaq Elite 8300 Desktop Computer with serial number MXL250153W and two USB drives discussed herein. G. KUIPER agreed to speak with officers. He said that there was nothing on the USB drives. G. KUIPER was asked if he had a cell phone. He admitted he had a cell phone and directed the Agents to the location of the cell phone that is one of the Devices. Also during the search warrant a second cellular telephone, separate from the aforementioned cell phone was discovered. When asked about the second cell phone G. KUIPER indicated he

had not utilized the second cell phone in quite some time.[10] Preliminary analysis of the second phone conducted in the presence of G. KUIPER indicated that the last phone call made on that cell phone was sometime during December, 2019. Agents did not seize the second cellular phone.

67. Additionally during the search warrant at the subject premises multiple computers were found. It was apparent several of the computers had not been utilized in quite some time and these computers were older model computers. G. KUIPER was asked what computer he utilized to conduct his online business and he directed agents to a desktop computer, the HP Compaq Elite 8300 Desktop Computer with serial number MXL250153W, located in a room labeled by the Agents as "Office." KUIPER indicated he did not have a laptop. Agents only seized the computer KUIPER identified as the computer he used for his online business and did not seize the older modeled computers.

68. Furthermore, G. KUIPER admitted during his consensual interview that he also utilizes public computers such as the Lawrenceville Public Library, and a computer located in a retail establishment around the corner from the Subject Premises. G. KUIPER indicated he utilizes the public computers primarily to read, and send personal emails.

69. Each of the devices was transported from the Subject Premises to the HSI offices at the Norris Cotton Federal Building in Manchester, New Hampshire. FDA-OCI maintains office space within the HSI offices. Each of them had been secured at the subject premises and packed all together in a United Parcel Service box for mailing from Georgia to the aforementioned location in New Hampshire. I know that they have been stored in such a way that they have not been tampered with and are in the same condition as when they were seized

[10] In various emails I reviewed, G. KUIPER provided his cell phone to customers and suppliers indicating it was used to discuss the illicit business.

due to the fact that the shipping box was still secured and did not appear to have been tampered with.

TRAINING AND EXPERIENCE CONCERNING ITEMS TO BE SEIZED

70. Based on my training and experience participating in cases involving the illegal distribution of prescription drugs via the internet, I know that websites that sell such drugs commonly represent themselves to customers as legal sellers of prescription drugs, including controlled substances, even though they dispense prescription drugs to customers who do not have valid prescriptions for the drugs. Such websites typically allow their customers to choose the drugs they want to purchase instead of requiring a licensed medical practitioner to determine the appropriate treatment based upon an evaluation of the customer's symptoms, medical history and other factors that a legitimate medical practitioner would consider before making a diagnosis and formulating a treatment plan. Some websites do not ask any health questions and do not require a prescription before illegally dispensing prescription drugs.

71. I know based upon my training and experience that individuals operating businesses out of their personal residences, even businesses engaged in illegal activity, maintain records such as invoices, purchase and sales agreements, financial documents such as money owed to and by the business, bank records, and records of customers and suppliers payments such as Western Union, Money Gram, Bank-to-bank wire transfers, and other records of payments. I know that these records are maintained not only in paper form, such as printouts, bound books, notepads, and pieces of paper, but also in the form of electronic storage such as computer disks, thumb drives, mobile telephone devices, and computer hard drives. Oftentimes, individuals maintain these records on their premises for long periods of time despite their

potential value as evidence in a criminal investigation. They do this in furtherance of the business and are oftentimes unaware of the records' potential incriminating nature.

72. Persons involved in illegal prescription drug sales almost always keep records of their transactions. On several occasions, I have observed such evidence in various forms including electronically stored on computers and/or storage devices.

73. The following types of items are often associated with the sales and/or laundering of illegal drug profits and are often found on electronic storage devices: bank records or evidence of large quantities of U.S. currency; daily worksheets, tally sheets or ledger sheets prepared by subjects in illegal prescription drug sales detailing the amounts of money or illegal drugs distributed; U.S. Postal shipping receipts documenting the receipt and/or shipment of packages via the U.S. mail; notes, ledgers, bank statements, money orders/Western Union/Money Gram payment receipts; wire transfer records; other records documenting the receipt/distribution of prescription drugs; other records documenting the receipt of payment related to the receipt/distribution of prescription drugs, as well as packaging and shipping materials.

74. Based on my training and experience and the training and experience of other agents with whom your affiant has worked, books, records, receipts, notes, ledgers, bank statements, money orders, cashier checks, passbooks, certificates of deposit, photographs, travel records, shipping receipts, bank records, and other documentation evidencing the obtaining, secreting, transfer, concealment or expenditure of proceeds acquired illegally are typically maintained by individuals participating in the above described criminal conduct in various forms, including paper documents, computer printouts, or on electronic storage devices.

75. I submit that there is probable cause to believe those records will be stored on the Devices, for at least the following reasons:

a. Based on my knowledge, training, and experience as well as my discussions with agents involved with computer forensics, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache".

e. Based on actual inspection of other evidence related to this investigation, spreadsheets, financial records, and invoices, I am aware that computer equipment was used to generate, store, and possibly print documents used in the criminal activity that is the subject of this investigation.

76. Forensic Evidence. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them and when. There is probable cause to believe that this forensic electronic evidence will be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and

events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in

advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

77. I submit that this affidavit supports probable cause for a warrant to search the Devices described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

/s/ Jason Rameaka

Jason Rameaka
Special Agent
FDA/Office of Criminal Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P.4.1 and affirmed under oath the content of this application and affidavit

Date: **Jul 10, 2020**

Time: **10:36 AM, Jul 10, 2020**

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PREMISES TO BE SEARCHED

The property to be searched includes:

a. one LG Brand flip phone;

b. one HP Compaq Elite 8300 Desktop Computer with serial number MXL250153W; and

c. two USB drives evidence number 09-0373-42156 one of which is labeled "Wincleaner" and one of which is labeled "rabbitTV."

Together, these will be referred to as "the Devices." The Devices are currently located in secure evidence storage in the custody of the FDA OCI located at the Norris Cotton Federal Building, 275 Chestnut Street, Manchester, New Hampshire.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEIZED

a. Information associated with the sale or importation of any unapproved new drugs and/or misbranded drugs, originating either from a foreign location or from within the United States, including prescription drugs that are also classified as controlled substances, including pay-owe sheets, buyer lists, telephone lists, address books, seller lists, ledgers, records of sales, records of expenditures made to purchase drugs, and records of expenditures to purchase products which are used in the distribution of drugs from 2010 to the present;

b. lists of customers and related identifying information;

c. types, amounts, and prices of sales as well as dates, places, and amounts of specific transactions;

d. any information related to suppliers of the drugs (including names, addresses, phone numbers, or any other identifying information);

e. any information involving the travel to obtain controlled substances or the transportation of controlled substances; records of shipments and customs forms;

f. information reflecting contact or communication with coconspirators, the distribution of controlled substances to coconspirators, and the disposition of proceeds of controlled substances (including within messaging applications like stored on telephones like iPhones);

g. all bank records, checks, credit card bills, account information, and other financial records;

h. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. I seek to seize records from 2010 to the present.

ATTACHMENT C

The search is related to a violation of the following offenses:

1. 21 USC 331(a), 331(d) – Introduction of Misbranded and Unapproved New Drugs into Interstate Commerce;

2. 21 USC 841(a), 846 – Distribution and Conspiracy to Distribute Controlled Substances;

3. 21 USC 952(b), 963 – Unlawful Importation of Controlled Substances;

4. 18 USC 371, 545 – Conspiracy and Importation Contrary to Law; and

5. 18 USC 1957, 1956(a)(2), and 1956(h) – Money Laundering.